Detector decoy quantum key distribution

Tobias Moroder[1,2], Marcos Curty[3] and Norbert Lütkenhaus[1,2]

[1] Quantum Information Theory Group, Institute of Theoretical Physics I, and Max-Planck Research Group for Optics, Photonics and Information, University Erlangen-Nuremberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany

[2] Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Canada

[3] ETSI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Campus Universitario, E-36310 Vigo, Spain

E-mail: tmoroder@iqc.ca

Abstract. Photon number resolving detectors can enhance the performance of many practical quantum cryptographic setups. In this paper, we employ a simple method to estimate the statistics provided by such a photon number resolving detector using only a threshold detector together with a variable attenuator. This idea is similar in spirit to that of the decoy state technique, and is specially suited for those scenarios where only a few parameters of the photon number statistics of the incoming signals have to be estimated. As an illustration of the potential applicability of the method in quantum communication protocols, we use it to prove security of an entanglement based quantum key distribution scheme with an untrusted source without the need of a squash model and by solely using this extra idea. In this sense, this *detector decoy method* can be seen as a different conceptual approach to adapt a single photon security proof to its physical, full optical implementation. We show that in this scenario the legitimate users can now even discard the double click events from the raw key data without compromising the security of the scheme, and we present simulations on the performance of the BB84 and the 6-state quantum key distribution protocols.

1. Introduction

Among the research performed nowadays in order to increase the secret key rate and distance that can be covered by quantum key distribution (QKD) systems, one can distinguish three main work areas which are closely related to each other [1, 2, 3]. On the one hand, we have the development of new proof techniques, together with better classical post-processing protocols, that are able to further extend the proven secure regimes for idealized QKD schemes, typically based on the transmission of two-level quantum systems (qubits) [4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. On the other hand, we find the continuous improvements that come from the technological side. Especially, the design of better light sources and better detectors should give us provable secure communications over a growing distance [14, 15, 16]. Finally, we have the research which aims to close the gap between theoretical security concepts for idealized QKD schemes and their experimental realization [17, 18, 19, 20, 21, 22, 23].

The awareness of such a theory-experiment gap was triggered by the important deviations present in practical QKD setups with respect to their original theoretical proposal, which usually demands technologies that are beyond our present experimental capability. Especially, the signal states emitted by the source, instead of being single photons, are usually weak coherent pulses which can contain more than one photon prepared in the same polarization state. Now, the eavesdropper (Eve) is no longer limited by the no-cloning theorem [24], since the multiphoton pulses provide her with perfect copies of the single photon. In this scenario, she can perform the so-called *photon-number splitting* attack [25, 26]. This attack gives Eve full information about the part of the key generated from the multiphoton signals, without causing any disturbance in the signal polarization. The use of weak coherent pulses jeopardizes the security of QKD protocols, and lead to limitations of rate and distance that can be achieved by these techniques. For instance, it turns out that the BB84 protocol [27] with weak coherent pulses can give a key generation rate of order $O(\eta^2)$ [20, 21], where η denotes the transmission efficiency of the quantum channel.

A significant improvement of the secret key rate can be obtained when the hardware is slightly modified. In particular, by using the so-called decoy state method [17, 18, 19]. In this approach, the sender (Alice) varies, independently and at random, the mean photon number of each signal state sent to the receiver (Bob) by employing different intensity settings. Eve does not know the mean photon number of each signal sent. This means that the gain and the quantum bit error rate (QBER) of each signal can only depend on its photon number but not on the particular intensity setting used to generate it. From the measurement results corresponding to different intensity settings, it turns out that the legitimate users can estimate the gain and the QBER associated to each photon number state and, therefore, obtain a better estimation of the behavior of the quantum channel. This translates into an enhancement of the resulting secret key rate. The decoy state technique has been successfully implemented in several recent experiments [16, 28, 29, 30, 31], and it can deliver a key generation rate of the same order of magnitude like single photon sources, *i.e.*, $O(\eta)$ [17, 18, 19].

The use of photon number resolving (PNR) detectors instead of threshold detectors can also enhance the performance of many practical QKD setups. For instance, in those situations where the decoy state method cannot be easily applied. This is the case, for example, in a QKD scheme with an untrusted source where the legitimate users cannot control the mean photon number of the signal states emitted. In these scenarios, it might be still very useful for the legitimate users to have access to the photon number statistics of the incoming signals. To simplify the security analysis, it is very tempting to assume a squash model for Alice's and Bob's detection setup [32]. This model maps each incoming signal to a one-photon polarization space followed by a measurement in this smaller dimensional Hilbert space. The squash model has been recently proven to be correct for the case of the BB84 protocol [33, 34]. However, in Ref. [34] it was shown that the same does not hold, for instance, for the active basis choice measurement in the 6-state protocol [35].

In this paper, we analyze a simple method to estimate the photon number statistics provided by a PNR detector using only a practical threshold detector together with a variable attenuator. The basic idea consists in measuring the incoming light field with a set of simple threshold detectors with different efficiencies and thus one obtains more information about the underlying distribution of the photons. This technique has its origin in the field of quantum metrology as discussed in Refs. [36, 37, 38] and has been successfully implemented in some recent experiments [39, 40, 41] which show the practical feasibility of the method. Here we apply it for the first time to various realistic QKD scenarios. For instance, it can be used to prove security of those QKD setups that do not have a squash model [34], or in those security proofs that only require the statistics given by a PNR detector [42]. However if one likes to employ this technique in the QKD context one has to estimate the photon number statistics under the worst case assumption for Alice and Bob. Thus the known reconstruction method from Refs. [37, 38] which considers only a truncated version of the problem (under the additional constraints of only a finite, small number of experimental runs) cannot be directly used for the QKD setups. Nevertheless, the central idea of the problem remains unchanged. In fact, this method can be considered as the decoy state technique applied to the detector side: If Alice and Bob vary, independently and at random, the detection efficiency of their apparatus then they can estimate the photon number statistics of the signals received. Note that the photon number distribution of the incoming signals cannot depend on the particular efficiency setting used to measure them. Therefore, from now on, we shall refer to this estimation procedure as *detector decoy* to emphasize its connection and applicability to QKD. The detector decoy idea can be employed both for calibrated and uncalibrated devices [3]. The essential requirement here is that Eve cannot modify the variable attenuator employed by the legitimate users to vary the detection efficiency of their setups.

Specifically, we apply the detector decoy method to two different QKD scenarios. In the first one, we prove the security of an entanglement based QKD scheme with an untrusted source solely by using this estimation procedure. More precisely, we investigate the situation where Alice and Bob perform either the BB84 or the 6-state protocol, and we compare the resulting key rates with those arising from a security proof based on the squash model assumption [32]. In contrast to this last scenario, now Alice and Bob can now even sift out the double click events without compromising the security of the scheme. Note, however, that we compare different situations, since they require different detection setups. As a second potential application, we analyze an alternative experimental technique, also based on the detector decoy method, to estimate the photon number statistics of the output signals in a "Plug & Play" configuration [14, 43, 44].

The paper is organized as follows. In Sec. 2 we describe in detail the detector decoy idea to estimate the photon number statistics of an optical signal by means of a threshold detector combined with a variable attenuator. Next, we apply this method to different practical QKD scenarios. In particular, Sec. 3 analyzes the security of an entanglement based QKD scheme with an untrusted source. Then, in Sec. 4 we propose an experimental technique to estimate the photon number statistics of the output signals in a "Plug & Play" configuration. Finally, Sec. 5 concludes the paper with a summary.

2. Estimating photon number statistics

Most of the security proofs for QKD only require the estimation of a few parameters related with the photon number statistics of the incoming signals. These parameters suffice to obtain good lower bounds for the achievable secret key rate. Here we discuss and explain the technique to measure the photon number distribution of an optical signal by means of a practical threshold detector in combination with a variable attenuator. As mentioned this idea has been introduced previously in the scientific literature before, cf. Refs. [36, 37, 38]. The current discussion differs in the particular way of how one reconstructs part of the photon number distribution from the observed measurement outcomes; here we need to provide ultimate bounds for certain photon number parameters, cf. Prop. 2.1, that are valid without any further assumptions on the signal states. Of course, the photon number distribution can also be obtained by using directly PNR detectors [45, 46]. This approach would provide Alice and Bob not only with the distribution of the incoming signals but also with the number of photons contained in each of them. Unfortunately, most of the methods proposed so far in the literature to construct this type of detectors result in devices with low detection efficiencies and which are unable to operate at room-temperatures. An interesting alternative is that based on detection schemes which use, for instance, time multiplexing techniques [47, 48]. This method has allowed, for example, a passive decoy selection in QKD, cf. Ref. [49, 50]. In this last case, however, the achievable photon number resolution depends on the number of detectors and on the number of spatially, or temporal, separate bins used.

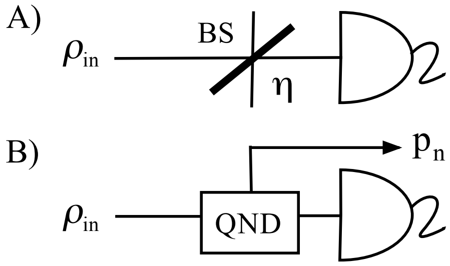

Figure 1. Case A) Detection setup which combines a beam splitter of transmittance η together with an ideal threshold detector. The incoming signal state ρ_{in} is given by Eq. 2. Case B) If one varies the transmittance η of the beam splitter, then the detection setup given in Case A is equivalent to a *quantum non-demolition* (QND) measurement that provides only the photon number statistics of the incoming signals.

The basic idea of the detector decoy technique can be highlighted with a simple example. Let the optical signals arriving to a *perfect* threshold detector be either a single photon pulse or a strong pulse containing several photons. These two signals will always produce a single click in the detector. Therefore, in this scenario both events cannot be distinguished. Suppose now that a beam splitter with very low transmittance is placed before the detector and the same kind of signals is received once more. Then, the single photon pulse will produce much less clicks than the strong pulse. In principle, both events can now be distinguished. That is, by varying the transmittance of the beam splitter more information about the photon number distribution of the signals received becomes available.

Let η denote the transmittance of such a beam splitter (Case A in Fig. 1). The combined detection setup can be characterized by a positive operator value measure (POVM) which contains two elements, $F_{\rm vac}(\eta)$ and $F_{\rm click}(\eta)$, given by [51]

$$F_{\rm vac}(\eta)=\sum_{n=0}^{\infty}(1-\eta)^n\Pi_n, \tag{1}$$

and $F_{\rm click}(\eta)=\mathbb{1}-F_{\rm vac}$, where Π_n represents the projector onto the n-photon subspace. That is, the outcome of $F_{\rm vac}(\eta)$ corresponds to no click in the detector, while the operator $F_{\rm click}(\eta)$ gives precisely one detection click, which means at least one photon is detected. Suppose for the moment that the input signal state is of the form

$$\rho_{\rm in}=\sum_{n=0}^{\infty}p_n\rho_n, \tag{2}$$

where the signals ρ_n belong to the n-photon subspace.

The probability of getting a click, that we shall denote as $p_{\rm click}(\eta)$, depends on the transmittance η of the beam splitter. It can be calculated as $p_{\rm click}(\eta)={\rm tr}[F_{\rm click}(\eta)\rho_{\rm in}]$. Similarly, $p_{\rm vac}(\eta)=1-p_{\rm click}(\eta)$ represents the probability that the detector does not click. Using Eq. 1, we find that this last quantity can be expressed as $p_{\rm vac}(\eta)=\sum_{n=0}^{\infty}(1-\eta)^np_n$. Now one can follow a similar idea to that of the decoy state method. In particular, if the receiver varies the transmittance $\eta=\{\eta_1,\ldots,\eta_M\}$ of the beam splitter he can generate a set of linear equations with the probabilities p_n as the unknown parameters [36, 37, 38],

$$\begin{aligned}p_{\rm vac}(\eta_1)&=\sum_{n=0}^{\infty}(1-\eta_1)^np_n,\\ &\vdots\\ p_{\rm vac}(\eta_M)&=\sum_{n=0}^{\infty}(1-\eta_M)^np_n.\end{aligned} \tag{3}$$

From the observed data $p_{\rm vac}(\eta)$, together with the knowledge of the transmittance η used, the receiver can solve Eq. 3 and obtain the value of p_n. For instance, in the general scenario where he employs an infinity number of possible decoy transmittances $\eta\in[0,1]$, he can always estimate any finite number of probabilities p_n with arbitrary precision. This result is illustrated as Case B in Fig. 1. On the other hand, if the receiver is only interested in the value of a few probabilities p_n, then he can estimate them by means of only a few different decoy transmittances, like in the decoy state method [17, 18, 19, 52]. This last statement is given by Proposition 2.1 for the case where the receiver only wants to find worst case bounds for the probabilities p_0, p_1, and p_2. This proposition can straightforwardly be generalized to cover also the case of any other finite number of probabilities p_n. Note, however, that it only constitutes a possible example of an estimation procedure that provides the exact values of the probabilities p_n in the considered limit. In principle, many other estimation techniques are also available, like linear programming tools [53] or different ideas from the original decoy state method [54].

Proposition 2.1. *[Finite settings] Consider the set of linear equations given by*

$$f(c) = \sum_{n=0}^{\infty} c^n x_n, \tag{4}$$

where the unknown parameters x_n fulfill $x_n \geq 0$ and $\sum_{n=0}^{\infty} x_n \leq C$ for a given constant C, and where c satisfies $c \in [0,1]$. Consider now three different settings $c_0 = 0$, c_1 and c_2. Then, the unknown variables x_0, x_1 and x_2 satisfy, respectively, $x_0 = f(c_0) = f(0)$,

$$l_1(c_1) = \frac{f(c_1) - f(0)\,(1-c_1^2) - c_1^2 C}{c_1 - c_1^2} \leq x_1 \leq u_1(c_1) = \frac{f(c_1) - f(0)}{c_1}, \tag{5}$$

and $l_2(c_1,c_2) \leq x_2 \leq u_2(c_1,c_2)$ with bounds

$$l_2(c_1,c_2) = \frac{f(c_2) - f(0)\,(1-c_2^3) - u_1(c_1)\,(c_2 - c_2^3) - c_2^3 C}{c_2^2 - c_2^3}, \tag{6}$$

$$u_2(c_1,c_2) = \frac{f(c_2) - f(0) - c_2 l_1(c_1)}{c_2^2}. \tag{7}$$

When $c_1 = \Delta$ and $c_2 = \sqrt{\Delta}$, the given bounds converge to the exact value of the variables x_1 and x_2 in the limit $\Delta \to 0$.

Proof. We present the explicit derivation of the upper bound $u_1(c_1)$ and of the lower bound $l_2(c_1,c_2)$. The other bounds can be obtained in a similar way. The basic idea is as follows: We first upper bound x_1 from the knowledge of $f(c_1)$; afterwards this result is used to lower bound x_2 given the value of $f(c_2)$. Starting with the definition of $f(c_1)$ we obtain

$$f(c_1) = x_0 + c_1 x_1 + \sum_{n=2}^{\infty} c_1^n x_n \geq f(0) + c_1 x_1, \tag{8}$$

where we have used the fact that $x_0 = f(0)$ and $x_n \geq 0$. This inequality already gives the upper bound $u_1(c_1)$ on x_1. To obtain the lower bound $l_2(c_1,c_2)$, note that the other extra condition on the open parameters x_n gives

$$\sum_{n=N+1}^{\infty} x_n \leq C - \sum_{n=0}^{N} x_n, \quad \forall N \in \mathbb{N}. \tag{9}$$

Using a similar inequality to that in Eq. 8 for the definition of $f(c_2)$ in combination with the condition given by Eq. 9 we obtain

$$\begin{aligned} f(c_2) &\leq x_0 + c_2 x_1 + c_2^2 x_2 + c_2^3 \left(C - x_0 - x_1 - x_2\right) \\ &\leq f(0)(1-c_2^3) + u_1(c_1)(c_2 - c_2^3) + x_2(c_2^2 - c_2^3) + c_2^3 C. \end{aligned} \tag{10}$$

In the second step we have employed again the fact that $f(0) = x_0$ together with the upper bound for $x_1 \leq u_1(c_1)$. Eq. 10 directly delivers the lower bound given by Eq. 6.

Let us now prove that both bounds converge. The unknown parameters x_n are exactly the Taylor expansion coefficients of the function $f(c)$ evaluated at the point $c = 0$, *i.e.*,

$$x_n = \frac{1}{n!} f^{(n)}(0) = \frac{1}{n!} \frac{d^n}{dc^n} f(c)\Big|_{c=0}. \tag{11}$$

This means that the upper bound $u_1(c_1)$ becomes exact if one finds the appropriate setting to estimate the first derivative. Choosing $c_1 = \Delta$ directly gives

$$\lim_{\Delta \to 0} u_1(\Delta) = \lim_{\Delta \to 0} \frac{f(\Delta) - f(0)}{\Delta} = f^{(1)}(0) = x_1. \tag{12}$$

For the lower bound $l_2(c_1, c_2)$ one has to perform the limit $c_1 \to 0$ prior to $c_2 \to 0$. Hence, one selects the setting $c_2 = \sqrt{\Delta} > \Delta = c_1$. Using the Taylor expansion series,

$$f(c_1) = f(\Delta) \quad \approx f(0) + f^{(1)}(0)\Delta, \tag{13}$$

$$f(c_2) = f(\sqrt{\Delta}) \approx f(0) + f^{(1)}(0)\sqrt{\Delta} + \frac{1}{2} f^{(2)}(0)\Delta, \tag{14}$$

we obtain

$$\begin{aligned} \lim_{\Delta \to 0} l_2(\Delta, \sqrt{\Delta}) = &\lim_{\Delta \to 0} \frac{1}{1 - \sqrt{\Delta}} \left\{ \frac{1}{2} f^{(2)}(0) + \sqrt{\Delta} \left[f(0) - C + f^{(1)}(0) \right] \right\} \\ &= \frac{1}{2} f^{(2)}(0) = x_2. \end{aligned} \tag{15}$$

This proves that also the lower bound on x_2 becomes exact in the considered limit. □

For the further discussion we shall assume that one can always obtain the exact values of the probabilities p_n, hence we will ignore any finite size effects from now on.

So far, we have analyzed the case of an ideal threshold detector. When the detector has some finite detection efficiency η_{det} and shows some noise in the form of dark counts which are, to a good approximation, independent of the incoming signals, such a detector can be described by a beam splitter of transmittance η_{det} combined with a noisy detector [55]. In this scenario the argumentation presented above still holds, and the detector decoy method can also be used in the calibrated device scenario. Note that the operator $F_{\text{vac}}(\eta)$ is now given by

$$F_{\text{vac}}(\eta) = (1 - \epsilon) \sum_{n=0}^{\infty} (1 - \eta\eta_{\text{det}})^n \Pi_n, \tag{16}$$

where ϵ represents the probability to have a dark count. In this case, $p_{\rm vac}(\eta)$ has the form

$$p_{\rm vac}(\eta) = (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta\eta_{\rm det})^n p_n. \tag{17}$$

Again, if one varies η then, from the measured data $p_{\rm vac}(\eta)$ together with the knowledge of the parameters η, $\eta_{\rm det}$ and ϵ, the receiver can deduce mathematically‡ the value of the probabilities p_n.

The results provided in this section rely on the description of the detectors given by Eq. 1 and Eq. 16. However, there are many different ways to model the exact behavior of an imperfect detector, and quite often the model is adapted to the explicit situation for which one wants to use the calculated data. The probability of a no click outcome given by Eq. 3 and Eq. 17 describes the typical QKD situation quite accurate (see, *e.g.*, Ref. [56]). Of course, whenever this situation changes the exact analysis need to be adapted. Nevertheless, the main idea behind the detector decoy method stays invariant. Via the observations on several different input distributions $\{p_n(\eta)\}$, that directly depend on the incoming photon number distribution $\{p_n\}$ by means of an explicit, known transformation rule (binomial transformation in the case of the beam splitter) one can obtain more information about the incoming photon statistics.

3. Entanglement based QKD schemes with an untrusted source

In this section we combine the detector decoy idea with the security statement for an entanglement based QKD scheme with an untrusted source. The schematic setup of the experiment is shown in Fig. 2. The source, which is assumed to be under Eve's control, is placed between the two receivers. In the ideal case, this source produces entangled states that are sent to Alice and Bob. The entanglement is contained in the polarization degree of freedom of the light field. This means that at least two different optical modes have to be considered for each side. On the receiving side, we assume that both measurement devices only act onto these two modes. For simplicity, we restrict ourselves to the familiar active polarization measurement setup, in which each party actively chooses the measurement basis β. In the BB84 protocol each receiver can choose between two different basis, while in the 6-state protocol all three different polarization axis can be selected. Each measurement device consists of a polarizing beam splitter that spatially separates the two incoming modes according to the chosen polarization basis β, followed by two threshold detectors on the two different output modes of the beam splitter. The analysis for other measurement devices, like for example a passive measurement setup is completely analogous. Entanglement based schemes constitute a very promising alternative to implement QKD over long distances. In fact, they hold the theoretical

‡ Note that the convergence result given in Proposition 2.1 does not apply directly to this scenario. However, it is still correct if one ignores the detector efficiency part. This is the case considered in Sec. 3, when we analyze the security of QKD schemes.

distance record for a QKD scheme without quantum repeaters so far, cf. the simulation in Ref. [32]. This type of protocols have been successfully implemented in many different recent experiments (See, *e.g.*, Ref. [57, 58, 59] and references therein.), and they are a suitable candidate to realize earth-satellite QKD links [60]. For more details on the setup, or on the measurement apparatus, we refer the reader to Refs. [32, 56].

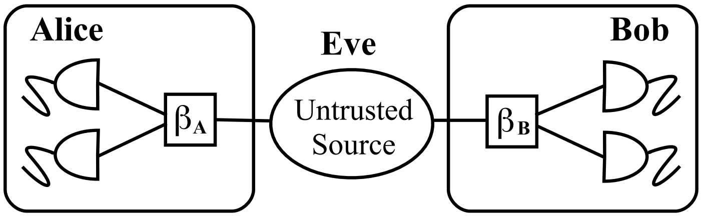

Figure 2. Schematic diagram of an entanglement based QKD scheme with an untrusted source for the case of an active choice of the measurements basis β_A, β_B respectively.

Section 3.1 includes the security analysis for an entanglement based QKD scheme. We follow the security proof technique provided in Ref. [12, 13, 23]. Using this approach allows us to directly pinpoint the usefulness of the detector decoy method in the security proof. The main result of Sec. 3.1 is given by Eq. 29, which shows that the final lower bound on the secret key rate only depends on a few essential parameters of the system. Then, in Sec. 3.2 we employ the detector decoy idea to estimate these parameters for the active measurement scheme. Finally, Sec. 3.3 contains the simulation of a real QKD experiment. There, we compare the detector decoy method with other proof techniques.

3.1. Secret key rate

We discuss the security level in the case of collective attacks. More precisely, we assume that the three parties Alice, Bob and Eve share an unlimited number of copies of the *same* state $|\Psi\rangle_{\mathrm{ABE}}$. Once Alice and Bob have received their part of the quantum state, they measure it to obtain information about the state $\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{E}}\left(|\Psi\rangle_{\mathrm{ABE}}\langle\Psi|\right)$. The POVMs used by Alice and Bob are denoted, respectively, as $\{F_i^{\mathrm{A}}\}$ and $\{F_j^{\mathrm{B}}\}$. They contain *all* the measurement operators that Alice and Bob perform during the protocol, *i.e.*, they also include the detector decoy measurements. These additional measurements enable the legitimate users to estimate some of the crucial parameters of the key rate formula with high confidence. Let us further assume that all the measurement operators are invariant under a projection measurement of the total number of photons [56]. That is, each of the elements F_i^{A} or F_j^{B} satisfies

$$F_i = \sum_{n=0}^{\infty} \Pi_n F_i \Pi_n. \tag{18}$$

Using this assumption, one can consider a slightly different, but completely equivalent, scenario for the distribution of the quantum states. The new scenario has the advantage that it allows a direct application of a known key rate formula based on unidirectional classical error correction and privacy amplification [12, 13, 23]. Proposition 3.1, however, holds independently of whether we restrict ourselves to unidirectional or bidirectional classical communication protocols in the post-processing stage.

Proposition 3.1. *Whenever Alice and Bob use photon number diagonal measurement devices, then the secret key rate in the following two scenarios is the same:*

(i) Eve distributes pure quantum states $|\Psi\rangle_{\mathrm{ABE}}$ *from a given set* $\mathcal{P}$ *which contains the purifications of the states* $\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{E}}(|\Psi\rangle_{\mathrm{ABE}}\langle\Psi|)$ *that are compatible with the observed measurement data.*

(ii) Alice, Bob and Eve share tripartite states $\rho_{\mathrm{ABE}} = \mathrm{tr}_{\mathrm{R}}(|\Phi\rangle_{\mathrm{ABER}}\langle\Phi|) \in \mathcal{S}$ *which originate from a four-party state of the form*

$$|\Phi\rangle_{\mathrm{ABER}} = \sum_{n,m=0}^{\infty} \sqrt{p_{nm}}|\phi_{nm}\rangle_{\mathrm{ABE}}|n,m\rangle_{\mathrm{R}}, \tag{19}$$

where $|\phi_{nm}\rangle_{\mathrm{ABE}}$ *represents a state that contains* n *photons in the mode destined to Alice and* m *photons in the mode for Bob, and where* $|n,m\rangle_{\mathrm{R}}$ *denotes an inaccessible shield system that records the photon number information of Alice and Bob's signals. The set of possible tripartite states* $\mathcal{S}$ *contains all such states for which the bipartite (photon-number diagonal) states* $\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{ER}}(|\Phi\rangle_{\mathrm{ABER}}\langle\Phi|)$ *are compatible with the observations.*

Proof. We show that for any state $|\Psi\rangle_{\mathrm{ABE}} \in \mathcal{P}$ chosen from the first scenario, there is a particular three party state $\rho_{ABE} \in \mathcal{S}$ from the second case such that Eve's position, once Alice and Bob have performed their measurements, is completely equivalent. The reverse direction of this statement holds trivially since $\mathcal{S} \subset \mathcal{P}$. Note that Eve's eavesdropping capabilities are completely determined by the collection of conditional states ρ_{E}^{ij} and their corresponding probabilities p_{ij}, both defined via the relation

$$p_{ij}\rho_{\mathrm{E}}^{ij} = \mathrm{tr}_{\mathrm{AB}}\left(F_i^{\mathrm{A}} \otimes F_j^{\mathrm{B}} \sigma_{\mathrm{ABE}}\right), \tag{20}$$

when Alice, Bob, and Eve share a state σ_{ABE}. Let us start with the first case, where $\sigma_{\mathrm{ABE}} = |\Psi\rangle_{\mathrm{ABE}}\langle\Psi|$ with $|\Psi\rangle_{\mathrm{ABE}} \in \mathcal{P}$. Using Eq. 20 and Eq. 18 we arrive at

$$\begin{aligned} p_{ij}\rho_{\mathrm{E}}^{ij} &= \sum_{n,m} \mathrm{tr}_{\mathrm{AB}}\left(\Pi_n^{\mathrm{A}} F_i^{\mathrm{A}} \Pi_n^{\mathrm{A}} \otimes \Pi_m^{\mathrm{B}} F_j^{\mathrm{B}} \Pi_m^{\mathrm{B}}\, |\Psi\rangle_{\mathrm{ABE}}\langle\Psi|\right) \\ &= \sum_{n,m} p_{nm}\, \mathrm{tr}_{\mathrm{AB}}\left(F_i^{\mathrm{A}} \otimes F_j^{\mathrm{B}} |\phi_{nm}\rangle_{\mathrm{ABE}}\langle\phi_{nm}|\right). \end{aligned} \tag{21}$$

In the second line we define $\Pi_n^{\mathrm{A}} \otimes \Pi_m^{\mathrm{B}}|\Psi\rangle_{\mathrm{ABE}} = \sqrt{p_{nm}}|\phi_{nm}\rangle_{\mathrm{ABE}}$. To compare it with the second scenario we select $|\Phi\rangle_{\mathrm{ABER}}$ arising from the state $|\Psi\rangle_{\mathrm{ABE}}$ via a coherent photon number measurement. Its outcome is stored in the additional register system R and the state is given by

$$|\Phi\rangle_{\mathrm{ABER}} = \sum_{n,m} \Pi_n^{\mathrm{A}} \otimes \Pi_m^{\mathrm{B}}|\Psi\rangle_{\mathrm{ABE}}|0\rangle_{\mathrm{R}} = \sum_{n,m} \sqrt{p_{nm}}|\phi_{nm}\rangle_{\mathrm{ABE}}|n,m\rangle_{\mathrm{R}}. \tag{22}$$

Using $\sigma_{\text{ABE}} = \text{tr}_{\text{R}}\left(|\Phi\rangle_{\text{ABER}}\langle\Phi|\right)$ in Eq. 20 directly delivers the same result as Eq. 21. This finally proves the proposition. □

Next we focus on a security proof that only requires direct classical communication in the reconciliation part of the protocol. More precisely, we apply the secret key rate formula derived in the recent security proof presented in Refs. [12, 13, 23]. It relies on Alice, Bob, and Eve sharing signal states of the form given by Eq. 19. Once the legitimate users have measured their part of $\rho_{\text{ABE}} = \text{tr}_{\text{R}}(|\Phi\rangle_{\text{ABER}}\langle\Phi|)$, they only have access to their classical outcomes which are stored in registers X and Y respectively. On the contrary, Eve still has at her disposal a quantum state. This scenario is described by the so-called ccq state $\rho_{\text{XYE}} = \mathcal{M}(\rho_{\text{ABE}})$ that results from the map

$$\rho_{\text{ABE}} \mapsto \rho_{\text{XYE}} = \mathcal{M}(\rho_{\text{ABE}}) = \sum_{i,j} p_{ij}|i,j\rangle_{\text{XY}}\langle i,j| \otimes \rho_{\text{E}}^{ij}, \tag{23}$$

where the probabilities p_{ij} and the conditional states $\rho_E^{i,j}$ are defined like in Eq. 20 by setting $\sigma_{\text{ABE}} = \rho_{\text{ABE}}$. According to Refs. [23], the secret key rate, that we shall denote as R, satisfies

$$R \geq \inf_{\rho_{\text{ABE}}\in\mathcal{S}} \sum_{n,m=0}^{\infty} g_{nm} S(X|E,n,m) - gH(X|Y). \tag{24}$$

The infimum runs over all possible tripartite states ρ_{ABE} that belong to the class $\mathcal{S}$ defined in Proposition 3.1. Here $H(X|Y)$ stands for the conditional Shannon entropy of Alice's random variable X conditioned on Bob's random variable Y. This part accounts for the error correction step of the protocol and it is independent of the chosen tripartite state $\rho_{\text{ABE}} \in \mathcal{S}$. In order to compute the conditional von Neumann entropies $S(X|E,n,m)$ describing Eve's information about Alice's raw key, we first calculate the ccq states for the definite photon number states $|\phi_{nm}\rangle_{\text{ABE}}$ as they appear in the decomposition $\rho_{\text{ABE}} = \sum_{n,m} p_{nm}|\phi_{nm}\rangle_{\text{ABE}}\langle\phi_{nm}| \in \mathcal{S}$. Let us denote these conditional ccq states as $\rho_{\text{XYE}}^{nm} = \mathcal{M}(|\phi_{nm}\rangle_{\text{ABE}}\langle\phi_{nm}|)$. From the definition of the conditional entropy we obtain $S(X|E,n,m) = S(\rho_{\text{XE}}^{nm}) - S(\rho_{\text{E}}^{nm})$, where $S(\rho)$ denotes the von Neumann entropy of a generic quantum state ρ. The remaining parameters that appear in Eq. 24 are the overall gain g and the individual gains g_{nm}, *i.e.*, the probability that Alice and Bob obtain an overall conclusive result when n and m photons are detected on each side respectively. These parameters can be written as

$$g_{nm} = p_{nm} Y_{nm}, \tag{25}$$

$$g = \sum_{n,m} g_{nm}, \tag{26}$$

with the conditional yields Y_{nm} defined as the probability that both parties obtain a conclusive outcome conditioned on the fact that they received a state $\text{tr}_{\text{E}}(|\phi_{nm}\rangle_{\text{ABE}}\langle\phi_{nm}|)$.

The detector decoy idea does not imply any change in the underlying security proof. In fact, one could even improve the lower bound on the secret key rate formula given in Eq. 24 by including local randomization steps [12, 13, 61, 62] or by allowing several rounds of classical bidirectional communication [23]. The main advantage of the detector decoy method is that it allows Alice and Bob to acquire more information about the class $\mathcal{S}$ over which they have to perform the optimization. As explained in the next subsection, one can in principle obtain the *full statistics* that PNR detectors could give. Note, however, that when Alice and Bob use PNR detectors they also have single shot resolution. Still, to have access to the statistics of the arriving signals allows the legitimate users to gain more knowledge about Eve's information on the raw key. Thus a smaller amount of privacy amplification is needed, and consequently one obtains more secret key.

One can further simplify the lower bound on the secret key rate formula such that only a few parameters need to be estimated, cf. Ref. [23]. The conditional entropies satisfy $H(X|n,m) \geq S(X|E,n,m) \geq 0$ for all photon numbers n and m. This means that the secret key rate R can always be lower bounded by restricting the sum in Eq. 24 to any of its items. For instance, one can select the single photon and the vacuum contributions only, and obtains

$$\begin{aligned} R \geq \inf_{\rho_{\mathrm{ABE}} \in \mathcal{S}} \sum_{m=0}^{\infty} g_{0m} S(X|n=0,m) + g_{11} S(X|E,n=1,m=1) \\ - g H(X|Y). \qquad (27) \end{aligned}$$

So far we have not considered any explicit QKD scheme yet. In the following we restrict ourselves to the BB84 and the 6-state protocols, since they allow us to express both entropies by means of quantities that are directly observable. Moreover, and for simplicity, let us assume that the sifted key is only composed by those events for which Alice and Bob have used their normal detection device, *i.e.*, all possible decoy outcomes are considered as inconclusive results and they are only used to estimate the class $\mathcal{S}$. Similarly, all the no click outcomes and all detection events where Alice and Bob employed different basis choices are discarded as well. In the case of double clicks two options are possible: Either they are discarded as well, or one assigns at random one of the two conclusive outcomes "0" or "1" [56]. As a result, Alice and Bob are left with binary values whenever they consider an outcome pair as conclusive. As shown in Ref. [12, 13], both parties can randomly flip their bit values together, which results in an overall symmetric error rate that gives $H(X|Y) = h_2(Q)$, where h_2 denotes the binary entropy. Any conclusive result on Alice's side that originates from a vacuum input contains no information for the eavesdropper [63]. If we assume that these events are completely unbiased we obtain $S(X|E,n=0,m) = 1$ for all m. This means that Alice and Bob do not need to perform any privacy amplification on all these outcomes, but note as well that they do not provide any key information because of the error correction part in the formula. The total *vacuum gain* is given by $g_0 = \sum_m g_{0m}$. The conditional von Neumann entropy from the single photon contribution can always be lower bounded by the completely symmetric case, which gives $S(X|E,n=1,m=1) \geq f(Q_{11})$, where f denotes a convex function that depends on the chosen protocol, and Q_{11} represents the conditional single photon QBER that one observes with *perfect* detectors. For the two considered protocols this function f takes the form §

$$f(x) = \begin{cases} 1 - h_2(x) & \text{BB84,} \\ 1 + h_2(x) - h_2(\frac{3x}{2}) - \frac{3x}{2}\log_2(3) & \text{6-state.} \end{cases} \qquad (28)$$

Let $g_{11}^{\min}$ and $g_0^{\min}$ denote lower bounds on the single photon and vacuum gain respectively, while $Q_{11}^{\max}$ represents an upper bound to the maximal attainable value of the single photon QBER, of all states compatible with the class $\mathcal{S}$. With this notation, the secret key rate satisfies

$$R \geq g_0^{\min} + g_{11}^{\min} f(Q_{11}^{\max}) - gh_2(Q), \qquad (29)$$

with the distinction between the BB84 and the 6-state protocol being only in the function f given by Eq. 28. Note that the gains g_{11}, g_0 and g depend on the choice of which outcomes are considered as conclusive. This decision includes as well the overall sifting effect. Let q denote the probability that both parties use their normal detection device and they measure in the same basis. Then, using an asymmetric basis choice in the setup in combination with a very rarely switching to the decoy measurement, this overall sifting factor q can be made arbitrary close to unity [64] and thus we can drop it in the evaluation section.

3.2. Detector decoy estimation

In this section we apply the detector decoy method to the active measurement setup as it is used in the usual BB84 or the 6-state protocol, and we show how Alice and Bob can estimate the essential quantities to evaluate Eq. 29. That is, the vacuum gain g_0, the single photon gain g_{11} and the conditional quantum bit error rate Q_{11} from perfect detectors.

The discussion starts with the typical model of an imperfect threshold detector which shows some noise in the form of dark counts as given by Eq. 17 with $\eta = 1$. Furthermore we require that Alice's and Bob's detectors have equal (and constant) detector inefficiency; otherwise this opens the possibility for powerful new eavesdropping attacks [65, 66] and other techniques have to be applied [67, 68]. Under this assumption it is a common technique to include the inefficiency of the detectors into the action of the quantum channel, and one performs the analysis with a threshold detector model of perfect efficiency. If one can prove security without knowing the exact detector efficiency, then one automatically also shows security with this particular extra

§ Let us mention two important points here. Because of convexity of both functions one could alternatively use the actual, single photon QBER as an argument of the lower bound functions. This situation corresponds to the case in which one assumes the uncalibrated device scenario for the evaluation of the privacy amplification part. However, if one takes into account any imperfections from the actual detection device, then one could even enhance the actual lower bound f. For example, if one considers a dark count model that randomly flips the bit value on Alice side (dark counts produce double clicks which are randomly assigned afterwards) this actually reduces Eve's information on the raw key and hence the privacy amplification part [12, 13]. Nevertheless we shall ignore this effect in our discussion.

knowledge. Suppose that both threshold detectors on each side have equal dark count probabilities. The POVM elements for the active measurement choice β are given by [56]

$$F_0 = (1-\epsilon)\sum_{n=1}^{\infty} |n,0\rangle_\beta\langle n,0| + \epsilon(1-\epsilon)|0,0\rangle\langle 0,0|, \tag{30}$$

$$F_1 = (1-\epsilon)\sum_{n=1}^{\infty} |0,n\rangle_\beta\langle 0,n| + \epsilon(1-\epsilon)|0,0\rangle\langle 0,0|, \tag{31}$$

together with $F_{\rm vac} = (1-\epsilon)^2|0,0\rangle\langle 0,0|$ and $F_{\rm D} = \mathbb{1} - F_{\rm vac} - F_0 - F_1$, with $F_{\rm D}$ denoting the operator associated with double click events. Here $|n,0\rangle_\beta$ and $|0,n\rangle_\beta$ refer to the corresponding two-mode Fock state in the chosen polarization basis β. Although we restrict ourselves to this particular model, the analysis that follows can also be straightforwardly adapted for the calibrated device scenario.

Let us begin by analyzing the single photon gain g_{11}. Consider a simple setup where Alice and Bob insert only a single beam splitter in front of their measurement devices. This beam splitter is of course not assigned to the quantum channel. This scenario is illustrated in Fig 3, where the transmittance of Alice and Bob's beam splitter is denoted as $\eta_{\rm A}$ and $\eta_{\rm B}$ respectively. This setup has the advantage that both legitimate users only need to collect the count rates for one variable beam splitter per site, but it still enables Alice and Bob to obtain the overall photon number distribution p_{nm} of the incoming signals. With this information they can directly compute the individual gain of the single photon contribution g_{11} for the considered scenarios. For this detection device the overall "no click" operator on Alice's side becomes

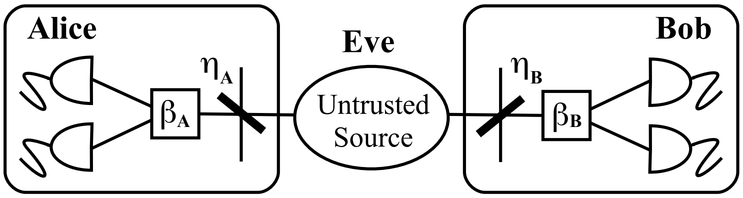

Figure 3. Schematic diagram of the first detector decoy setup considered. Alice and Bob place a single beam splitter, with transmittance η_A and η_B respectively, in front of their detection device.

$$F^{\rm A}_{\rm vac}(\eta_{\rm A}) = (1-\epsilon)^2\sum_{n=0}^{\infty}(1-\eta_{\rm A})^n\Pi^{\rm A}_n, \tag{32}$$

where the projector onto the n-photon subspace is given by

$$\Pi^{\rm A}_n = \sum_{k=0}^{n} |k,n-k\rangle_\beta\langle k,n-k|. \tag{33}$$

Note that this operator is independent of the chosen measurement basis $\vec{\beta}$, and hence we omit this label in the following whenever it is redundant. A similar expression holds for Bob's measurement operator $F_{\mathrm{vac}}^{\mathrm{B}}(\eta_{\mathrm{B}})$. Suppose that both parties receive now the generic input state ρ_{AB}, then they observe a no click outcome with probability

$$p_{\mathrm{vac}}^{\mathrm{AB}}(\eta_{\mathrm{A}},\eta_{\mathrm{B}}) = (1-\epsilon)^4 \sum_{n,m=0}^{\infty} (1-\eta_{\mathrm{A}})^n (1-\eta_{\mathrm{B}})^m p_{nm}, \tag{34}$$

where the photon number distribution p_{nm} is given by $p_{nm} = \mathrm{tr}_{\mathrm{AB}}(\Pi_n^{\mathrm{A}} \otimes \Pi_m^{\mathrm{B}} \rho_{\mathrm{AB}})$. Now, if Alice and Bob vary the transmittance of their inserted beam splitters, they can generate a whole set of linear equations similar to those given by Eq. 34, in which the photon number distribution p_{nm} appears as the open parameter. With this set of equations the whole distribution becomes accessible to Alice and Bob, however if they are only interested in the single photon probability p_{11} then the three different settings of Proposition 2.1 are already enough. Next, let us compute the single photon gain g_{11} for two different scenarios. Whenever Alice and Bob randomly assign bit values to their double click outcomes any single photon state will necessarily produce a conclusive outcome. In the second case, we consider that only single clicks contribute to the raw key rate. Here the individual gain is slightly lower than in the first situation since a single photon can trigger a double click event because of dark counts. The two different individual gains are given, respectively, by

$$g_{11,\mathrm{d}} = p_{11}, \tag{35}$$

$$g_{11,\mathrm{s}} = (1-\epsilon)^2 p_{11}, \tag{36}$$

where the subscripts "d" (with double clicks) and "s" (single clicks only) label the two different cases. Let us mention that the idea of obtaining the impinging photon number statistics with only one variable beam splitter can as well be applied to other photon number preserving linear networks, since the probability to obtain an overall no click outcome in the all the threshold detectors after such a network can always be calculated by replacing the whole network by only one such threshold detector.

The vacuum gain g_0 represents a direct observable quantity even without the detector decoy method. It only relies on the fact that one can obtain the statistics of a perfect threshold detector from the observed data of a detector which has dark counts [69]. Suppose that Bob considers a specific measurement outcome k which he can perfectly distinguish with his measurement device, and the corresponding POVM element is denoted by F_k^{B}. Then, the probability that Alice registers no click at all while Bob sees this specific outcome is given by

$$p_{\mathrm{vac},k}^{\mathrm{AB}} = (1-\epsilon)^2 \, \mathrm{tr}_{\mathrm{AB}} \left(|0,0\rangle_{\mathrm{A}}\langle 0,0| \otimes F_k^{\mathrm{B}} \rho_{\mathrm{AB}} \right) = (1-\epsilon)^2 p_{0\mathrm{k}}. \tag{37}$$

Since both parties can have access to the dark count probability ϵ they can directly use Eq. 37 to compute the probability $p_{0,\mathrm{k}}$ from perfect threshold detectors. Using this value directly allows to infer the vacuum gain for the two different scenarios as

$$g_{0,\mathrm{d}} = [1-(1-\varepsilon)^2] p_{0,\mathrm{d}}, \tag{38}$$

$$g_{0,\mathrm{s}} = 2\epsilon(1-\epsilon) p_{0,\mathrm{s}}. \tag{39}$$

The resolved single photon QBER Q_{11} is *inaccessible* with the simple detector decoy setup presented above. We can consider a more complicated setup in which a variable beam splitter is place in front of each threshold detector. This scenario is depicted in Fig. 4. Now Alice and Bob can adjust the transmittance of their two beam splitters $\vec{\eta}_{\rm A} = (\eta_{{\rm A},1}, \eta_{{\rm A},2})$ and $\vec{\eta}_{\rm B} = (\eta_{{\rm B},1}, \eta_{{\rm B},2})$ respectively. Although, from a practical point of view, this scenario is less attractive than the previous one—it requires a more complicated statistical analysis—it is interesting on a conceptual level since it can provide Alice and Bob with the same statistics like PNR detectors. Obviously all the results from the simple setup apply if one selects $\eta_{{\rm A},1} = \eta_{{\rm A},2} = \eta_{\rm A}$ and similar for Bob's side. Now the POVM element for the overall no click outcome on Alice's side is given by

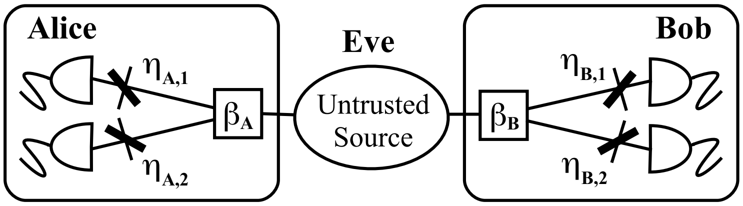

Figure 4. Schematic diagram of the second scenario analyzed, where Alice and Bob place a variable beam splitter in front of every threshold detector.

$$F^{\rm A}_{{\rm vac},\beta_{\rm A}}(\vec{\eta}_{\rm A}) = (1-\epsilon)^2 \sum_{k,l=0}^{\infty} \bar{\eta}^k_{{\rm A},1} \bar{\eta}^m_{{\rm A},2} |k,l\rangle_{\beta_A}\langle k,l|, \tag{40}$$

where we use the abbreviation $\bar{\eta} = 1 - \eta$. A similar expression can be obtained for $F^{\rm B}_{{\rm vac},\beta_{\rm B}}(\vec{\eta}_{\rm B})$. In contrast to the first measurement device analyzed, now the no click outcome depends on the chosen polarization basis $\vec{\beta} = (\beta_{\rm A}, \beta_{\rm B})$. The probability of the combined "no click" outcome in Alice's and Bob's side can be written as

$$p^{\rm AB}_{{\rm vac},\vec{\beta}}(\vec{\eta}_{\rm A}, \vec{\eta}_{\rm B}) = (1-\epsilon)^4 \sum_{k,l,r,s=0}^{\infty} \bar{\eta}^k_{{\rm A},1} \bar{\eta}^l_{{\rm A},2} \bar{\eta}^r_{{\rm B},1} \bar{\eta}^s_{{\rm B},2}\; q_{\vec{\beta}}(k,l;r,s), \tag{41}$$

where the probabilities $q_{\vec{\beta}}(k,l;r,s)$ have the form

$$q_{\vec{\beta}}(k,l;r,s) = {\rm tr}_{\rm AB}\left(|k,l\rangle_{\beta_{\rm A}}\langle k,l| \otimes |r,s\rangle_{\beta_{\rm B}}\langle r,s|\; \rho_{\rm AB} \right). \tag{42}$$

These probabilities coincide with the ones provided by PNR detectors. Using again the idea of different settings for the transmittance of the adjustable beam splitters one can generate more linear equations of the form given by Eq. 41. Consequently, the photon number resolved statistics $q_{\vec{\beta}}(k,l,r,s)$ become accessible to Alice and Bob. With this resolved distribution at hand it is straightforward to compute the single photon QBER $Q_{\vec{\beta},11}$ that Alice and Bob would observe using perfect detectors. It is determined by

$$p_{11} Q_{\vec{\beta},11} = q_{\vec{\beta}}(1,0;0,1) + q_{\vec{\beta}}(0,1;1,0). \tag{43}$$

Note that one has to use the symmetrized single photon QBER in the lower bound formula given by Eq. 29.

3.3. Evaluation

In this part we evaluate the lower bound on the secret key rate for the different decoy detection schemes presented in the last subsection. Additionally, we compare it with a security proof that relies on the validity of the squash model; for a different comparison between the squash model and an alternative estimation procedure not based in this last paradigm see also Ref. [70]. We assume that all relevant parameters that appear in the lower bound formula can be estimated precisely, *i.e.*, we ignore any statistical effect of an estimation procedure that uses only a few number of decoy settings.

Suppose that the observed data originate from a pumped type-II down conversion source. The states emitted by this type of source can be written as [71]

$$|\Psi_{\text{source}}\rangle_{\text{AB}} = \sum_{n=0}^{\infty} \sqrt{p_n} |\Phi_n\rangle_{\text{AB}}, \tag{44}$$

where the probability distribution p_n is given by

$$p_n = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{45}$$

The parameter λ is related with the pump amplitude of the laser and determines the mean photon pair number per pulse as $\mu = 2\lambda$. Each signal state $|\Phi_n\rangle_{\text{AB}}$ contains exactly $2n$ photons; n of them travel to Alice and the other n to Bob. These states are of the form

$$|\Phi_n\rangle_{\text{AB}} = \sum_{m=0}^{n} \frac{(-1)^m}{\sqrt{n+1}} |n-m, m\rangle_{\text{A}} |m, n-m\rangle_{\text{B}}, \tag{46}$$

where we have used the standard basis on each side, *i.e.*, $\beta_{\text{A}} = \beta_{\text{B}} = z$. When $n = 1$, the signal state in Eq. 46 becomes the EPR state, which admits perfect anticorrelations in all directions‖. When $n \geq 2$, the states $|\Phi_n\rangle_{\text{AB}}$ represent W-states. That is, even if Alice and Bob measure them along the same direction they might observe double clicks. In fact, the biggest contribution in the observed QBER stems from the multiphoton pairs. For instance, if the signal $|\Phi_{n=2}\rangle$ loses only one photon in the channel, then the error rate of the resulting state (although still entangled) is already about¶ 16.6%. This QBER is above the threshold error rate allowed by the one-way security proof employed in the previous section, even assuming a single qubit realization. This means, in particular, that the expected average mean photon number λ which optimizes the secret key rate in the long distance limit is quite low, and one does not expect a security proof which enables to drive the source with a much higher mean photon number.

To generate the observed data of an experiment that uses this kind of source we employ the following procedure: Since the loss is the predominant factor in the error rate and in the overall gain, we assume that the state emitted by the source passes first

‖ If Alice and Bob employ the measurement devices from Eqs. 30, 31, then they would always observe anticorrelated outcomes. Hence, one of the parties has to interchange the observed data "0" ↔ "1".

¶ Note, however, that there are different, more complicated measurement techniques that can be more robust against particle loss from a PDC source [72].

through a lossy, but otherwise error-free channel. Such a channel is characterized by the loss coefficient α and the total distance l. We include as well in the channel the effect of the detector efficiency η_{det} of the measurement device. Hence, the overall transmission in the optical line towards Alice becomes

$$\eta_{\mathrm{A}} = \eta_{\mathrm{det}} 10^{-\frac{\alpha l}{10}} = 10^{-\frac{\mathrm{db_A}}{10}}, \tag{47}$$

and determines the overall loss coefficient $\mathrm{db_A}$. A similar relation holds also for the channel towards Bob. The total loss between both parties is characterized by $\mathrm{db_{tot}} = \mathrm{db_A} + \mathrm{db_B}$. After the lossy channel, we include the effect of the misalignment and the dark counts of the detectors in the observed data. The misalignment varies slightly the polarization of the incoming light field. This effect changes over time and it is assumed to be uncontrollable. Averaging it results in an action similar to that of a depolarizing channel. Specifically, we consider the following misalignment model: Every time a single photon arrives at the detection device it triggers the correct detector with probability $(1-e)$, while with probability e it changes its polarization and triggers the wrong detector. When more photons enter the detection apparatus this effect is assumed to occur independently for every single photon and hence it can also change the probability to observe a double click. To conclude, we assume as well that Alice's and Bob's detectors suffer from dark counts as described in the previous subsection. Dark counts are typically the crucial parameter that limit the distance of a QKD scheme.

Next, we compare the different lower bounds on the secret key rate for the various scenarios considered, which again are distinguished by the subscripts "s" and "d" depending on the double click choice. In the simple detector decoy setup the resolved error rate is not directly accessible. Still, one can upper bound it via a worst case assumption. That is, we consider that *all* errors originate from the single photons only. In the single click case this upper bound, denoted as $\overline{Q}_{11,\mathrm{s}}$, is given by[+]

$$\overline{Q}_{11,\mathrm{s}} = \frac{1}{g_{11,s}} \left(Q_{\mathrm{s}} g_{\mathrm{s}} - g_0 \frac{1}{2} \right) \geq Q_{11}. \tag{48}$$

A similar relation gives the upper bound $\overline{Q}_{11,\mathrm{d}}$ for the double click case. On the other hand, in the detector decoy scheme which has two variable beam splitters in each side the conditional quantum bit error rate Q_{11} is equal to the hypothetical QBER arising with perfect detectors, independently of the chosen scenario. The different lower bounds are illustrated in Tab. 1. This table also includes the case where both parties employ *perfect* PNR detectors. This type of detectors allows them to condition the error correction on the photon number observed. This way, the term $H(X|Y)$ which appears in Eq. 24 can be changed by the conditional term $\sum g_{nm} H(X|Y,n,m)$. The lower bound contained in Tab. 1 corresponds to the case where single click events are the only conclusive outcomes. A fair comparison with a security proof based on the squash model is only possible if one employs the result from Refs. [33, 34] to further extend the validity of the squash

[+] From this estimation one could even try to calculate out the dark count probability of the detectors. However, we shall ignore this effect here.

Scenario	Lower bound
Updated Squash	$\tilde{g}_0 + \tilde{g}_{11}[1 - h_2(\tilde{Q}_{11})] - g_{\rm d} h_2(Q_{\rm d})$
Double	$g_{0,{\rm d}} + g_{11,{\rm d}} f(Q_{11}) - g_{\rm d} h_2(Q_{\rm d})$
Double + Bound	$g_{0,{\rm d}} + g_{11,{\rm d}} f(\overline{Q}_{11,{\rm d}}) - g_{\rm d} h_2(Q_{\rm d})$
Single	$g_{0,{\rm s}} + g_{11,{\rm s}} f(Q_{11}) - g_{\rm s} h_2(Q_{\rm s})$
Single + Bound	$g_{0,{\rm s}} + g_{11,{\rm s}} f(\overline{Q}_{11,{\rm s}}) - g_{\rm s} h_2(Q_{\rm s})$
PNR	$p_{11}[f(Q_{11}) - h_2(Q_{11})]$

Table 1. Different lower bounds on the secret key rate for the various scenarios considered with active basis choice measurements.

model to the situation where Alice's and Bob's detectors have dark counts; otherwise one loses the vacuum gain. The exact target measurements are given by Eqs. 30, 31 with $n = 1$ and where every double click is randomly assigned to one bit value. As a result, we obtain the lower bound formula given in Tab. 1 ("Updated squash") in which $\tilde{g}_0$ and $\tilde{g}_{11}$ denote, respectively, the squashed vacuum gain and the corresponding single photon gain, while $\tilde{Q}_{11}$ stands for the conditional QBER on the squashed single photons. Since the squash model does not exist for the active 6-state protocol* [34], here one cannot choose the function f.

For the simulation we consider an asymmetric distance scenario, since this situation optimizes the gain of the detector decoy idea over a security proof that relies on the squash model. In particular, we assume that Bob is much closer to the source than Alice. Such a situation might appear often in a QKD network, where certain users can be further away from the relay stations than others. The results for the BB84 and the 6-state protocol are shown, respectively, in Fig. 5 and in Fig. 6. The first case always corresponds to the situation where Alice and Bob place a single beam splitter in front of their detection device, while the second case represents the scenario where the legitimate users place a variable beam splitter in front of every threshold detector. The position of the source is denoted by a black square and is kept constant at a $\mathrm{db_B} = 3$ loss distance, so we only increase the distance towards Alice. For each lower bound we perform an optimization over the free parameter λ that corresponds to the mean photon pair number.

It is worth mentioning that the squash model delivers a higher lower bound on the secret key rate than that corresponding to the detector decoy method in the double click case. This seems surprising at first since the detector decoy idea provides the

* All formulae in Tab. 1 are for active basis choice measurements. In particular in a passive basis choice selection the results of the squash model change. One could at least discard double or multiclick events between different basis outcomes, and moreover a squash model exists for the passive 6-state protocol.

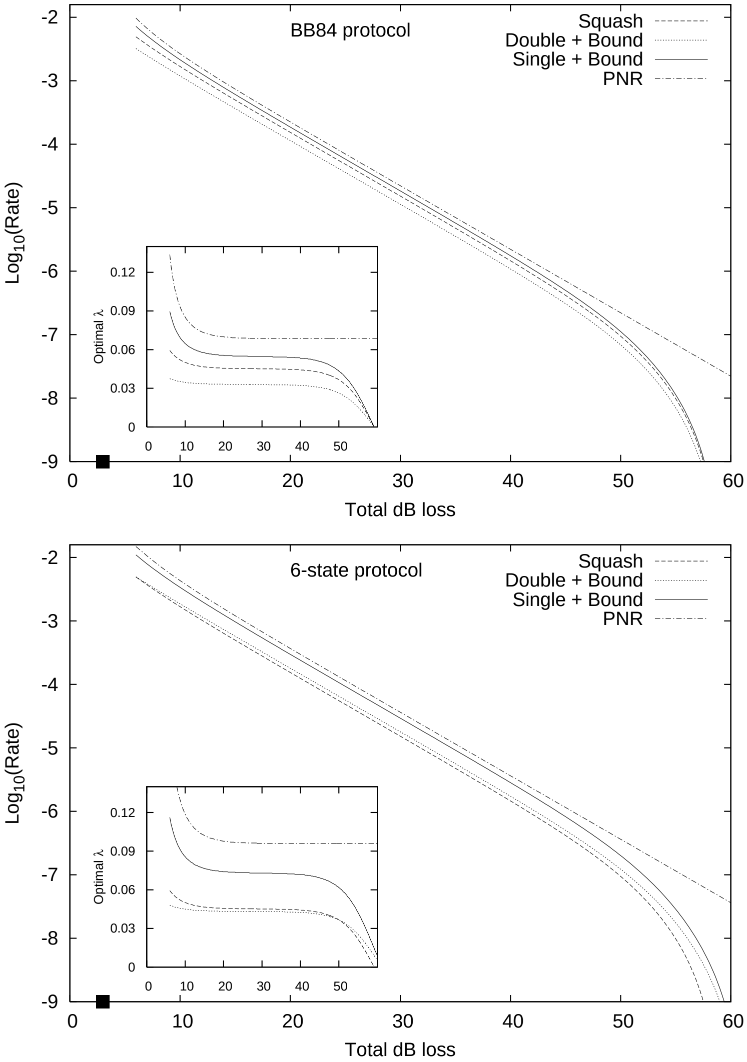

Figure 5. Different lower bounds on the secret key rate for the simple decoy detection setup shown in Fig. 3 with $\epsilon = 10^{-6}$ and $e = 0.03$. The inset figure shows the value for the optimized parameter λ of the source.

exact knowledge of all important single photon parameters. Note, however, that in the discussion which leaded to the lower bound formula given by Eq. 27 we restricted ourselves to only draw a secret key from the single photon contribution. In contrast, the squash model does not necessarily constrain the parties to obtain a secret key from the single photon contribution only, but instead attempts to even draw a secret key from the multiphoton events. In this sense, one can consider the squash model as a "calculation method" that allows to lower bound the amount of privacy amplification necessary for the multiphoton events by an equal amount of privacy amplification "calculated" on a hypothetical single photon state. Hence using the squash model directly lower bounds the key rate from Eq. 24. On the contrary, the detector decoy idea provides a slightly higher secret key rate than the squash model when Alice and Bob discard their double click events. Note that this action is not possible with the squash model assumption.

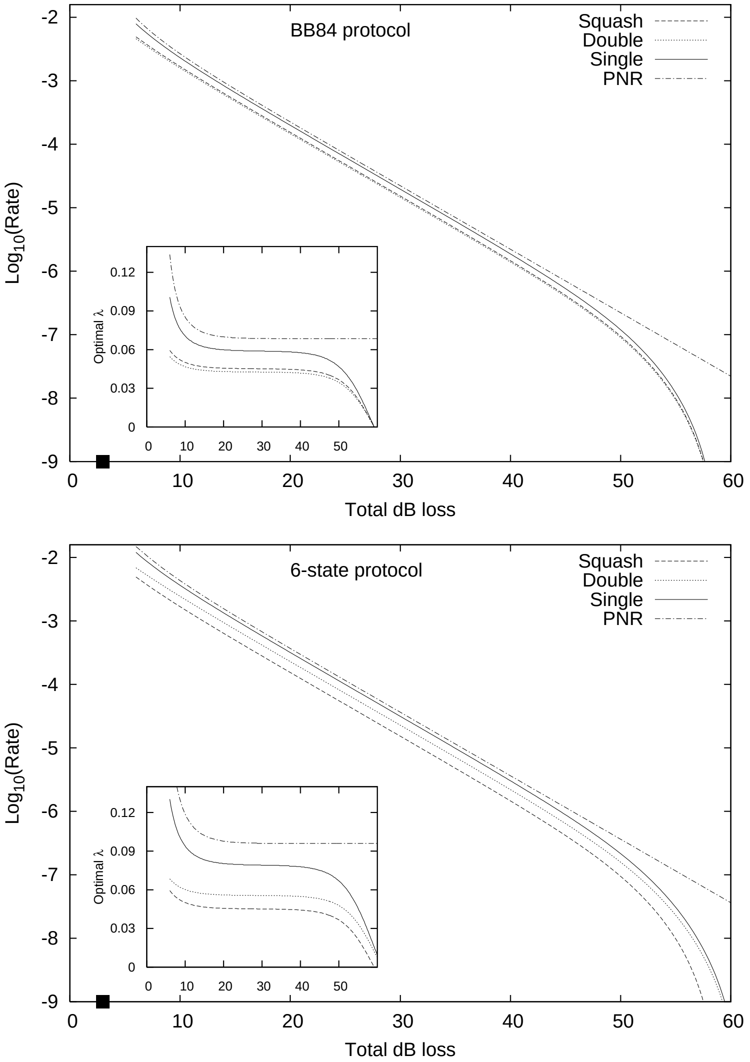

Figure 6. Different lower bounds on the secret key rate for the refined decoy detection setup shown in Fig. 4 with $\epsilon = 10^{-6}$ and $e = 0.03$. The inset figure shows the value for the optimized parameter λ of the source.

For the asymmetric distance scenario, this fact allows the two parties to drive the source with a slightly higher mean photon number, since the double clicks that occur frequently on the side closer to the source can be discarded from the error rate. See inset plots of the optimized mean photon number in Figs. 5, 6. In the squash model one has to keep the double click rate low on both sides, because the penalty in the error rate for each double clicks is 50%. Therefore, one has to use a lower mean photon number. This effect decreases with the distance, and in the long distance limit this advantage vanishes. Moreover, note that by adding the vacuum gain in the lower bound formula the resulting maximal achievable distance is shifted by around db = 10.

We have shown that the detector decoy idea provides a simple method to adapt a single photon security proof to its full optical implementation, while still providing similar key rates as those arising from a security proof using the squash model assumption. Its main advantage relies on the fact that it can be straightforwardly applied also to QKD protocols, like the active 6-state protocol, where the squash model, the other "adaption technique", does not work.

4. "Plug & Play" configuration

The main feature of the Plug & Play configuration for QKD is that it is intrinsically stable and polarization independent [14, 43, 44]. Apart from synchronization between Alice and Bob, no further adjustments are necessary. This fact renders this proposal a promising approach for commercial QKD systems.

Specifically, in this type of QKD schemes Bob sends to Alice a train of bright laser pulses through the quantum channel. On the receiving side, Alice first attenuates the incoming signals to a suitable weak intensity. Afterwards, she codes the secret key information using phase coding, and sends the resulting weak pulses back to Bob, who detects them. The main idea behind this bi-directional quantum communication design is that now the interferometers used in a practical implementation of the scheme are self-stabilized because the light passes through them twice. Moreover, if the reflection on Alices side is done by means of a Faraday mirror, then the polarization effects of the quantum channel can also be compensated.

A full security proof of a Plug & Play system has recently been given in Ref. [73]. However, the security analysis contained in Ref. [73] is based on a slightly modification of the hardware included in the original Plug & Play proposal. In particular, Alice performs three measures that enhance the security of the protocol and also simplify its investigation [73, 74]. First, she blocks any undesired optical mode by means of an optical filter. Then, she performs active phase randomization. This last action transforms the incoming signals into a classical mixture of Fock states. Finally, she measures the photon number distribution of the pulses received in order to estimate some bounds on the photon number statistics of the output signals. This can be done by randomly sampling the incoming pulses with an optical switch followed by an intensity monitor (Case A in Fig. 7). The beam splitter that appears in this figure is used to implement the decoy state method which improves the whole performance of the scheme. More recently, a similar proposal has also been analyzed [75]. Basically, it substitutes the optical switch with a passive beam splitter (Case B in Fig. 7).

In this section, we present very briefly an alternative experimental technique to estimate the photon number statistics of the output signals. It is based on the detector decoy idea presented in Sec. 2. Moreover, it allows Alice to perform the decoy state method simultaneously, *i.e.*, without using an additional variable beam splitter. The scheme is illustrated in Fig. 7 as Case C. It consists on a balanced Mach-Zehnder interferometer combined with a threshold detector. After the active phase randomization step performed by Alice, the signal states entering the interferometer are given by Eq. 2. Now, the probability that the threshold detector does not click is given

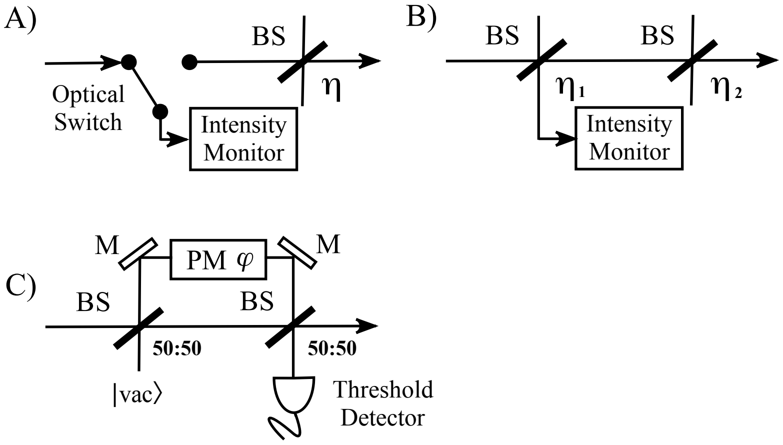

Figure 7. Case A) Schematic diagram of the detection setup employed by Alice to estimate the photon number statistics of the output signals. The variable beam splitter which appears in the figure implements the decoy state method [73]. Case B) Illustration of a more recent experimental proposal to achieve the same goal [75]. It uses a passive beam splitter together with an intensity monitor. Like before, the second beam splitter in the figure is used to realize the decoy state method. Case C) Alternative method based on one balanced Mach-Zehnder interferometer combined with a threshold detector. PM denotes a phase modulator, M represents a mirror, and $|\mathrm{vac}\rangle$ is a vacuum state.

by

$$p_{\mathrm{vac}}(\varphi)=\sum_{n=0}^{\infty}\left(\frac{1-\cos\varphi}{2}\right)^n p_n, \tag{49}$$

where φ represents the phase imprinted by the phase modulator of the interferometer. Like before, if Alice varies, independently and at random for each signal, the phase φ of her setup, then, from the observed probabilities $p_{\mathrm{vac}}(\varphi)$, together with the knowledge of the parameters $[(1-\cos\varphi)/2]^n$, she can estimate the photon number distribution p_n with high confidence. Given that the probabilities p_n are now known, Alice can also estimate the photon number statistics q_n of the output signals. These probabilities are given by

$$q_n=\sum_{m=n}^{\infty}\frac{m!}{n!(n-m)!}\frac{p_m}{2^m}(1-\cos\varphi)^n(1+\cos\varphi)^{m-n}. \tag{50}$$

Note that by varying the phase φ of her interferometer Alice also modifies simultaneously the photon number probabilities q_n of the output signals, as required in the decoy state method, without the need of an additional beam splitter to perform this task.

5. Conclusion and outlook

In this paper we have analyzed a simple technique which allows the direct application of a single photon security proof for quantum key distribution (QKD) to its physical, full optical implementation. This so-called detector decoy method is conceptually different to that of the squash model, the other adaptation mechanism. It is based on an estimation procedure for the photon number distribution of the incoming light field that uses only a simple threshold detector in combination with a variable attenuator. The detector decoy method is similar in spirit to that of the usual decoy state technique: Since the eavesdropper does not know the particular detection efficiency setting used to measure the signals, any eavesdropping attempt must leave the expected photon number distribution unchanged (similar to the conditional channel losses in the decoy state technique).

Specifically, we have investigated an entanglement based QKD scheme with an untrusted source where Alice and Bob actively choose the measurement basis of either the BB84 or the 6-state protocol. The security of both schemes is proven solely by means of the detector decoy method and without the need of a squash model, which would have to be proven to be correct for each measurement device anew. Besides, and opposite to the squash model paradigm, the detector decoy technique allows the legitimate users to discard double click events from the raw key data. As a result, it turns out that the secret key rates in the infinite (or sufficiently large) key rate limit of a BB84 simulated experiment are comparable with each other for both alternatives. However, the detector decoy idea offers a slightly better performance in those scenarios where there exists no squash model, like in the 6-state protocol. In any real-life QKD experiment much more obstacles have to be taken care of and thus the situation can change quite drastically, mainly because of finite size effects. Nevertheless, for the current increasing interest in examining the finite size behavior of different protocols, it can only be of advantage to have a broader spectrum of different proof techniques available, even if they all show a similar behavior in the asymptotic key rate limit. Finally, as another potential application of the detector decoy method in QKD, we have briefly described an experimental procedure to estimate the photon number statistics of the output signals in a "Plug & Play" QKD configuration. We believe there might be many other potential applications of this method in QKD, like for instance in Ref. [67]. In addition, it could also be used to estimate the single photon contribution in the two state protocol with a strong reference pulse [76, 42].

To conclude, let us mention that there might be scenarios where it is not really necessary to insert and vary the transmittance of an additional beam splitter in the measurement device. For instance, let us consider the efficient, passive BB84 measurement setup, in which a beam splitter of high transmittance $\eta = 1 - \Delta$ splits the incoming light in favor of one basis versus the other. With this measurement apparatus, one can obtain directly three different beam splitter settings to apply the detector decoy formalism: Using the overall "no click" outcome of all detectors gives $\eta_1 = 1$, whereas if one ignores all the outcomes of only one basis and looks at the no click outcomes in the other basis, then one obtains two more settings, $\eta_2 = 1 - \Delta$ and $\eta_3 = \Delta$. Although these three settings are different from the ones given in Proposition 2.1 they can still provide good estimations of the single photon contribution. Moreover, the method could be improved even further. After all, in showing security we have not used all available information from our measurement results, as the further occurrences of double or multiclicks in our detection devices has been ignored. The use of this extra knowledge can only enhance the estimation procedure and thus can further reduce the number of necessary detector decoy settings. In fact, it is possible to provide a BB84 security proof by just using an estimation technique [70]. It might be interesting to compare the detector decoy idea with the results presented in Ref. [70], and we leave these open questions for further analysis.

Acknowledgements

The authors wish to thank H.-K. Lo, W. Mauerer, K. Tamaki, X. Ma and J. Lavoie for very useful discussions, and in particular M. Genovese for pointing out important references. M. Curty especially thanks N. Lütkenhaus and H.-K. Lo for hospitality and support during his stay at the Institute for Quantum Computing (University of Waterloo) and at the University of Toronto, where this manuscript was finished. This work was supported by the European Projects SECOQC and QAP, by the NSERC Discovery Grant, Quantum Works, CSEC, by Xunta de Galicia (Spain, Grant No. INCITE08PXIB322257PR), and by University of Vigo (Program "Axudas á mobilidade dos investigadores").

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Dušek M, Lütkenhaus N and Hendrych M 2006 *Progress in Optics* vol 39 ed Wolf E (Elsevier) p 381

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M A framework for practical quantum cryptography arXiv.org:0802.4155

[4] Mayers D 1996 *Advances in Cryptology — Proceedings of Crypto '96* (Berlin: Springer) pp 343–357 available as quant-ph/9606003

[5] Mayers D 2001 *JACM* **48** 351–406

[6] Lo H K and Chau H F 1999 *Science* **283** 2050

[7] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[8] Chau H 2002 *Phys. Rev. A* **66** 060302(R)

[9] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theory* **49** 457

[10] Devetak I and Winter A 2005 *Proc. of the Roy. Soc. of London Series A* **461** 207

[11] Koashi M 2006 *J. Phys.: Conf. Ser.* **36** 98

[12] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

[13] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332

[14] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41

[15] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nature Photonics* **1** 343

[16] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503

[17] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 57901

[18] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[19] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[20] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quant. Inf. Comp.* **4** 325

[21] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J. D* **41** 599

[22] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[23] Kraus B, Branciard C and Renner R 2007 *Phys. Rev. A* **75** 012316

[24] Wooters W K and Zurek W H 1982 *Nature* **299** 802

[25] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863–1869

[26] Brassard G, Lütkenhaus N, Mor T and Sanders B 2000 *Phys. Rev. Lett.* **85** 1330

[27] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India* (New York) p 175

[28] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[29] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A and Weinfurter H 2007 *Phys. Rev. Lett.* **98** 010504

[30] Dynes J F, Yuan Z L, Sharpe A W and Shields A J 2007 *Optics Express* **15** 8465

[31] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118

[32] Ma X, Fung C F F and Lo H K 2007 *Phys. Rev. A* **76** 012307

[33] Tsurumaru T and Tamaki K Security proof for QKD systems with threshold detectors arXiv:0803.4226

[34] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Phys. Rev. Lett.* **101** 093601

[35] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–3021

[36] Mogilevtsev D 1998 *Opt. Commun.* **156** 307

[37] Rossi A R, Olivares S and Paris M G A 2004 *Phys. Rev. A* **70** 055801

[38] Zambra G and Paris M G A 2006 *Phys. Rev. A* **74** 063830

[39] Zambra G, Andreoni A, Bondani M, Gramegna M, Genovese M, Brida G, Rossi A and Paris M G A 2005 *Phys. Rev. Lett.* **95** 063602

[40] Genovese M, Gramegna M, Brida G, Bondani M, Zambra G, Andreoni A, Rossi A R and Paris M G A 2006 *Laser Physics* **16** 385

[41] Brida G, Genovese M, Gramegna G, Meda A, Olivares S, Paris M G A, Piacentini F, Predazzi E and Traina P A review on recent results on on/off reconstruction of optical states arXiv:0810.5472

[42] Tamaki K, Lütkenhaus N, Koashi M and Batuwantudawe J Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse, arXiv.org/quant-ph/0607082

[43] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793

[44] Ribordy G, Gautier J D, Gisin N, Guinnard O and Zbinden H 2000 *J. Mod. Opt.* **47** 517–531

[45] Cabrera B, Clarke R M, Colling P, Miller A J, Nam S and Romani R W 1998 *Appl. Phys. Lett.* **73** 735

[46] Kim J, Takeuchi S, Yamamoto Y and Hogue H H 1999 *Appl. Phys. Lett.* **74** 902

[47] Achilles D, Silberhorn C, Sliwa C, Banaszek K, Walmsley I A, Fitch M J, Jacobs B C, Pittman T B and Franson J D 2003 *Opt. Lett.* **28** 2387

[48] Lundeen J S, Feito A, Coldenstrodt-Ronge H, Pregnell K L, Silberhorn C, Ralph T C, Eisert J, Plenio M B and Walmsley I A Measuring measurement arXiv:0807.2444

[49] Mauerer W and Silberhorn C 2007 *Phys. Rev. A* **75** 050305(R)

[50] Mauerer W, Helwig W and Silberhorn C 2008 *Ann. Phys.* **17** 158

[51] Rohde P P and Ralph T C 2006 *J. Mod. Op.* **53** 1589

[52] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326

[53] Bazaraa M S, Jarvis J J and Sherali H D 2004 *Linear Programming and Network Flows* 3rd ed (New York, Chichester: John Wiley & Sons)

[54] Tsurumaru T, Soujaeff A and Takeuchi S 2008 *Phys. Rev. A* **77** 022319

[55] Yurke B 1985 *Phys. Rev. A* **32** 311

[56] Lütkenhaus N 1999 *Phys. Rev. A* **59** 3301

[57] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, Weier H, Scheidl T, Lindenthal M, Blauensteiner B, Jennewein T, Perdigues J, Trojek P, Ömer B, Füerst M, Meyenburg M, Rarity J, Sodnik Z, Barbieri C, Weinfurter H and Zeilinger A 2007 *Nature Physics* **3** 481

[58] Ling A, Peloso M P, Marcikic I, Scarani V, Lamas-Linares A and Kurtsiefer C Experimental quantum key distribution based on a bell test arXiv:0805.3629

[59] Erven C, Couteau C, Laflamme R and Weihs G Entangled quantum key distribution over two free-space optical links arXiv:0807.2289

[60] Ursin R and et al Space-QUEST: Experiments with quantum entanglement in space arXiv:0806.0945

[61] Renes J M and Smith G 2007 *Phys. Rev. Lett.* **98** 020502

[62] Smith G, Renes J M and Smolin J A 2008 *Phys. Rev. Lett.* **100** 170502

[63] Lo H K 2005 *QIC* **5** 5

[64] Lo H K, Chau F and Ardehali M 2005 *J. of Cryptology* **18** 133

[65] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313

[66] Qi B, Fung C H F, Lo H K and Ma X 2007 *QIC* **7** 73

[67] Fung C H F, Tamaki K, Qi B, Lo H K and Ma X Security proof of quantum key distribution with detection efficiency mismatch arXiv.:0802.3788

[68] Lydersen L and Skaar J Security of quantum key distribution with bit and basis dependent detector flaws arXiv:0807.0767

[69] Moroder T, Curty M and Lütkenhaus N 2006 *Phys. Rev. A* **73** 012311

[70] Koashi M, Adachi Y, Yamamoto T and Imoto N Security of entanglement-based quantum key distribution with practical detectors arXiv.org:0804.0891

[71] Kok P and Braunstein S L 2000 *Phys. Rev. A* **61** 042304

[72] Brassard G, Mor T and Sanders B C Quantum cryptography via parametric downconversion quant-ph/9906074

[73] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev. A* **77** 052327

[74] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320

[75] Peng X, Jiang H, Xu B, Ma X and Guo H Experimental quantum key distribution with an untrusted source arXiv:0806.1671

[76] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121